Installation and Auditing of Security Technology

Session IV: Technical and Policy Focus Groups
Group B

Peter J Crook*, Robert M Rodger,
Flight Sergeant Barry Connell RAF

Police Scientific Development Branch
Home Office
Langhurst House
Langhurstwood Road
Horsham
West Sussex
RH12 4WX
United Kingdom

Tel: +44 1403 255451
Fax: +44 1403 213827
Email: pcrook@langhurst.org.uk

Abstract
Successful organisations and companies aim at value for money in all aspects of their business, including security.

Concentrating mainly on equipment to improve an organisation's physical security will not necessarily ensure that the resulting system will be effective. Realistic performance criteria should be used in specifying countermeasures against existing and potential new threats. Serious thought should also be given to the training of the operators and the writing of clear and effective operating procedures.

Security system auditing against the identified requirements should be undertaken shortly after the system is installed then carried out regularly to ensure that the system continues to meet the performance requirements and therefore that the initial investment on the system is proving worthwhile.

This paper offers guidance on achieving value for money in procuring and installing a physical security system. It also describes the skills required to audit perimeter security systems. It uses lessons learnt from a diverse range of projects, including some from work directed towards protecting critical national infrastructures in the United Kingdom

Introduction
The Police Scientific Development Branch (PSDB) of the Home Office has for many years been advising, assisting and developing security strategies and technologies for industry and government use. This has meant working closely with the oil and gas industry, the power generation and distribution utilities, the water supply companies and with government departments. Work has been carried out with the Prison Service to enhance the security regimes within prisons.

In July 1996 President Clinton called into being the President's Commission on Critical Infrastructure Protection[1] (PCCIP) which reported in October 1997. This was to develop a strategic approach to the protection, both current and postulated, of the United States critical infrastructures. The PCCIP combined security expertise from both government and industry in the exercise. In the United Kingdom a similar exercise had been carried out many years previously, co-ordinated through the Cabinet Office, that has looked at Economic Key Points (EKP).

Several of the findings of the PCCIP correspond closely with our views. It may be argued that Britain is several years ahead of the US in the implementation of counter-terrorist measures and this paper is designed to share, from this perspective, some of our experiences.

Threat, Asset and Vulnerability

If an organisation decides to spend money on security, it should carry out some form of risk assessment to ensure that the money is spent wisely. So, as a first step, the organisation should determine its assets, the threats against them and the vulnerability of these assests to disruption. The organisation's managers should be realistic when addressing these issues, irrespective of the organisation's size or business area.

For each of the three areas; threat, asset and vulnerability, specific information should be sought and analysed:

1. Threat.
   What are the threats, their likelihood and frequency?

2. Asset.
   For each asset, what are the implications of loss both in terms of criticality and cost but also how easy is the assest to replace or bypass?

3. Vulnerability.
   What are the immediate and peripheral vulnerabilities of the assets?

Only when all three of these aspects are assessed can it be judged whether there is a security problem that needs addressing. A useful by-product of this Risk Assessment process is that a disaster recovery or contingency plan can be produced with little additional effort.

"A terrorist bomb is only one of a number of possibly disastrous threats which a business faces nowadays. In many respects a serious fire, flood, or a catastrophic failure of a company's IT infrastructure, may be as damaging to the business as the consequences of a bomb explosion. A Business Continuity Plan should be drafted in such a way as to cover all risks."[2]

"Managers are increasingly coming to recognise that disaster recovery planning is an essential function in the management of the business. This is not surprising. Studies have shown that about 80% of companies which do not have a workable recovery plan will fail within one year of suffering a major disaster."[2]

The British Government has been developing a methodology, known as "Baseline Measures" to improve value for money, reduce costs and make security more objective.

The baseline measures approach considers assets as tangible (information, equipment, people, buildings and commodities) and intangible (morale, reputation etc.). This methodology also considers threats as traditional (espionage, terrorism, theft, insider etc.) and non traditional (fire and flood). Thus a thorough and penetrating examination of a business's security needs can aid the long term survivability of that organisation.

Operational Requirement and Performance Specification

The procurement process should aim to deliver a system which matches the needs of the organisation. This should be carried out only after the risk assessment has been completed, and security enhancements are deemed necessary. The next step, after the high level risk assessment, is the development of specific operational requirements for specific assets or vulnerabilities.

An operational requirement (OR) can be defined as a statement of needs based on a thorough and systematic assessment of the problems to be solved and the required solutions[3]. But what does that mean? In PSDB, the OR methodology was initially designed to take prospective customers through the minefield of procuring closed circuit television (CCTV) systems for deployment in an urban environment. However, the concept can be applied to any form of procurement from paperclips to battle-tanks. It relies on a partnership between the customer and an OR facilitator to address the actual security problems, which may differ from the perceived problems.

The customer (this term may cover more than one project stakeholder) is taken through a series of questions relevant to the problem. We have developed question sheets for CCTV deployment in urban areas, military establishments and penal institutions. These prompt the customer to focus on specific issues and to decide whether or not they are relevant. It is essential that the OR is "customer driven" and that the facilitator acts as the "interpreter" of technical information that the customer may not fully understand. The facilitator must not offer "his" solution to the customer but remain detached from offering any opinions, no matter how well founded.

Once the OR has been written and all parties who have contributed to the production of the document have agreed on its format and content, the OR is given to the "technical expert". It is his or her job to translate the OR into a performance specification (PS). A PS is used to determine whether the performance of a system is sufficient to meet the needs of the OR. The PS should be based on objective and measurable figures of merit which relate to mandatory functions required by the OR. Included in the PS should be a set of measurable standards which fulfil two basic functions:

1. to help the potential contractor understand exactly what the customer requires; and
2. to provide a rejection mechanism if the end product does not conform adequately to the PS, i.e. to enable the customer to withhold payment, if that becomes necessary.

The PS should then be included in an Invitation to Tender (ITT) and sent out to selected contractors for them to offer their design solution to the problem and the relevant costings. Selection of the contractor to carry out the work should ideally be taken on merit, and not just cost.

Acceptance Tests

It should be ensured that throughout the system installation process, the Project Manager monitors progress by liaising with the Contractor. Before "accepting" the finished product, the customer must ensure that it has been installed correctly and performs in accordance with the performance specification based upon the operational requirement. This phase of the project is the acceptance or commissioning testing and is where the value of using measurable standards becomes evident.

The contractor should be clear that once he has stated that the system is ready for testing, any subsequent failure to meet the agreed standard may lead to the system being rejected. Included in the PS will be the standards to be tested, the levels to be achieved, the method of testing and the test equipment to be used. Choice of test equipment can sometimes be a contentious point with the contractor and customer each preferring to use their own instruments. It is essential that whichever instruments are used, that they should properly calibrated and certified as such. Multimeters should sample at the same rate and have the same features; lightmeters should be colour corrected (if applicable); a standard test target should be used for determining target height or picture resolution in a CCTV system, etc. Any failure to have or specify a test procedure gives the contractor the potential not to satisfy the PS, at no penalty.

> At one establishment a contractor had been requested to provide twelve cameras on poles in order to view the perimeter. The establishment was provided with exactly what they had asked for, twelve cameras on poles. However, the cameras were installed without power or any image transmission system. There was presumably an intimation of what was really required but because of the lack of a PS, the establishment did not have any means for rejection of this inadequate system. Further expense was incurred in order to remedy the situation.
>
> In contrast, PSDB placed a contract to install twenty eight cameras within a prison establishment. The installation had to be carried out to a high specification because the cameras were to be used with a sophisticated video motion detection system. When the installation failed the acceptance tests, the contractor was given the test information and the reasons for failure. After several attempts by the contractor to remedy the situation the contract was terminated. Excuses querying whether PSDB could expect a contractor to meet some of the requirements did not carry weight. The contractor had read and accepted the PS and had contractually agreed to meet the requirement. Another contractor was engaged to finish the installation.

Without testing against the measurables listed within a PS, the customer may be left with no option other than to accept a sub-standard system.

Equipment, People and Procedures

It is vital to understand that any security system is only as good as the elements that make it up. In addition to the equipment, such as detection systems, closed circuit television and lighting, there is a need for competent operators and well written procedures.

There is little point in deploying "state of the art" hardware, procured using a performance specification, without having carefully drawn up operational procedures. Nor can management expect an effective system where there is good hardware and procedures controlled by poorly trained or badly motivated operators.

System managers often lose sight of the importance of operator training. However, an operator's performance will be a key determining factor in the overall effectiveness of the system. PSDB has developed guidance[4] for the selection and training of operators of closed circuit television systems. The value of this guidance has been demonstrated in pilot trials.

Maintenance Testing and Auditing

Effective programmed maintenance can be carried out only if a maintenance contract or schedule has been set up.

> Q: Why do we need to maintain our system?
> A: To ensure that when required the system performs to meet the need.

The level of maintenance required should be identified in the OR and included in the PS. An effective maintenance schedule should comprise weekly, monthly, bi-annual and annual tasks carried out by a combination of technical and non technical personnel.

Just like the acceptance tests, specific aspects of performance should be measured against previously set standards. An audit is a series of checks, designed to test whether a system's performance meets the OR. The results of one audit should be comparable with previous test results, allowing managers to identify even a small deterioration in equipment performance. Any significant changes in results indicate that there is a problem to be addressed. Correcting these deficiencies when they are discovered protects system owners from the embarrassment of discovering a weakness during or after a "real" incident.

> An establishment which used CCTV cameras, placed within the sterile zone, around its perimeter had a camera which had failed. The camera was replaced by the contractor and the camera pole was re-erected. The view along a sterile zone looked very much the same regardless of which camera it was being viewed from. It was only during a maintenance test that it transpired the camera had been replaced

pointing the opposite way from the original. This created a whole zone where an attacker could have crossed without being seen.

Assuming that the customer's needs for the system have not changed then an audit team need be familiar only with the system PS. Audit teams should work rigorously and systematically through each of the tests required to be carried out. It is important that members of the audit team have no vested interest in the outcome of the audit. It is advisable for the team to be engaged from an outside organisation for tests. No special skills are required to conduct an audit but it is necessary that the team is fully able to conduct each separate test required and understands fully the implications of test failure. Familiarity with the system's function, before any tests are started, should speed up the auditing process and help to eliminate any errors. The audit team should report their work in writing, clearly and concisely and, if necessary, diplomatically.

Testing Systems

All parts of the security system, the equipment (barriers, detection systems, closed circuit television, security lighting and access control technology), the people (operators and response forces) and the procedures all need to be tested to confirm compliance with the customer needs. Only when the needs have been addressed and the security solutions have been appropriately implemented can we expect that "value for money" is to be obtained.

References

1) President's Commission on Critical Infrastructure Protection
1997

2) Business as Usual
Home Office
www.homeoffice.gov.uk

3) CCTV Operational Requirements Manual
J Aldridge
PSDB Publication 17/94

4) CCTV: Making it Work
Training Practices for CCTV Operators
C Diffley, E Wallace
PSDB Publication 9/98